BTR
F#2016R01560

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
----------X

IN THE MATTER OF AN APPLICATION
APPLICATION FOR A SEARCH WARRANT
FOR: A SILVER & WHITE, APPLE
IPHONE 6 ASSIGNED NUMBER
516-425-0224

AFFIDAVIT IN SUPPORT
OF A SEARCH WARRANT

M.J. No. 19-869

----------X
EASTERN DISTRICT OF NEW YORK, SS:

DAVID DARJANIA, being duly sworn, deposes and states that he is a Special Agent with the Internal Revenue Service – Criminal Investigation ("IRS-CI"), duly appointed according to law and acting as such:

Upon information and belief, there is probable cause to believe that there is located in A SILVER & WHITE APPLE IPHONE 6 ASSIGNED NUMBER 516-425-0224, IMEI: 359309060188473 AND UTILILIZED AND SEIZED FROM DEFENDANT LORRAINE SUE PILITZ (the "DEVICE") further described in Attachment A, for the items described in Attachment B, all of which constitute evidence, fruits and instrumentalities of filing false Federal tax returns, corrupt endeavor to obstruct and impede the Internal Revenue Laws and structuring financial transactions in violation of Title 26, United States Code, Sections 7201(1), 7212(a) and Title 31, United States Code, Section 5324.

The source of your deponent's information and the grounds for his belief are as follows:

1. I am a Special Agent with the Internal Revenue Service – Criminal Investigation. I have worked with the IRS-CI for 10 years. During my tenure at the IRS-CI,

I have participated in many investigations involving violations of Tax Laws, Bank Secrecy Act and other related offences. In the course of those investigations, I have analyzed various financial records, conducted physical surveillance, monitored undercover operations, interviewed and debriefed cooperating witnesses and confidential informants. As a result of my training and experience, I am familiar with the techniques and methods of operation used by individuals involved in such criminal activity to conceal their activities from detection by law enforcement authorities.

2. I am familiar with the facts and circumstances of this investigation from: (a) my personal participation in this investigation, (b) reports made to me by other law enforcement authorities, (c) interviews of witnesses, and (d) review of other records and reports.

3. Because this affidavit is being submitted for the purpose of establishing probable cause to search, I have not included every detail of every aspect of the investigation. Rather, I have set forth only those facts that I believe are necessary to establish probable cause. The information set forth below is based upon my experience and training as a law enforcement officer with the IRS-CI, my review of documents and other evidentiary items, debriefing of witnesses, and my discussions with other law enforcement agents.

BACKGROUND

4. Since February 2011, the Federal Taskforce comprised of IRS-CI Special Agents and Suffolk County Police Department ("SCPD") Detectives were assisting U.S. Attorney's Office ("USAO") with a Grand Jury investigation of a marijuana grow and distribution network that produced and distributed large quantities of hydroponically grown

marijuana and the related money laundering activity in the Eastern District of New York, including Nassau and Suffolk Counties.

5. In October 2013, during arraignment and bail hearing following an arrest of James W. Ford ("Ford"), one of the subjects of the above-stated activity, Lorraine Sue Pilitz, AKA Lorraine Christie, AKA Lorraine Storms, AKA L.S. Christie-Pilitz ("Pilitz") identified herself to the government as Ford's girlfriend and employer. Pilitz indicated that Ford was an "off the books" employee of her company. Pilitz represents herself as a sole owner and operator of several corporations/ companies that provide tow and auto-body repair services from several locations in Nassau and Suffolk Counties. Pilitz is alleged to have personal and business relationships with Ford, who was convicted of possession in excess of 5 pounds of hydroponically grown marijuana.

7. In May/June 2014, the IRS-CI, expanded the on-going narcotics and money laundering investigation to designate Pilitz as a subject of the investigation. In June 2014 IRS-CI Special Agents and SCPD Detectives conducted Search Warrants at several locations including Pilitz' residence, multiple business locations, and other locations believed to have contained evidence related to the ongoing investigation, including the investigation of potential tax violations (and other related offences) committed by Pilitz. During those Court ordered search warrants an Apple iPhone was seized from the defendant. A search of that iPhone obtained the following relevant evidence:

> Pilitz' cellphone contained multiple text messages to various associates describing her financial transactions and claiming she was "losing her business" and has "no money".
>
> In addition there were drug-related text messages sent to Pilitz by her acquaintances. For example:

On 3/27/2013 Pilitz received a texts,

> *"I'm gonna need the biggest fatty ever after this" and "Tell JIMBO [referring to FORD] I'm gonna need a Jumbo";*

On 4/18/2014 Pilitz received a text from her other acquaintance,

> *"Bring a bone".*

The telephone records and other information recovered from the Pilitz' cellphone also confirmed that Pilitz was associated with other drug dealers, such as Scott Hogan (Hogan) who was listed in the contacts as "Hogan Scottie." Hogan was a multi-ton marijuana dealer who served 10 years in federal prison for prior narcotics and money laundering convictions. He is believed to be currently active both in drug distribution and money laundering.

Pilitz' cellphone contained text messages sent to Hogan ("Hogan Scottie" at telephone number (917) 647-8006), and Ford (listed as "Jim Went Bad" at the telephone number (516) 978-4454) indicating her knowledge of Fords illegal activities, including the drug dealing. For example:

> *Don't talk to jimmy anymore he's very shity not very remorseful about our money[1] I'm losing the bus[iness] have no money to pay anyone him and Scott thk ther so smart I'll go to the fed a make the deal they both can rot in jail !!*

In addition, during a 11/15/2013 civil action deposition, Pilitz admitted to using her cellphone to conduct tow and auto-repair business (Pilitz , et. al. v. Village of Freeport, Village of Freeport Police Dep't., Village of Malverne and Village of Malverne Police Dep't. 12-CV-5655-JFB-ARL). The transcript of the deposition is approx. 300 pages and the telephone use was referenced on several instances. PILITZ stated that she used her cellphone to both make and receive telephone calls as well as to send and receive business-related text messages. For example:

> *Q: You said, sometimes, you'll take calls yourself after the night. How do you do that? Do you stay up all night? Do you just leave the phone by your bed?*
> *A: I would forward it on to my cell phone.*
> *Q: You would leave your cell phone by your bed?*
> *A: Yeah.*

---

[1] Agents believe this refers to Fords' drug proceeds, structured and used by Pilitz to purchase a garage in Lindenhurst, N.Y. Agents identified over one million dollars that was generated by the defendant Ford from drug sales. When Ford was convicted and imprisoned for possession of drugs his monies were no longer available to sustain the business.

Q: How do you differentiate between when you're going to be taking the phone calls at night and when you're going to be using the service? Do you have to call the service ahead of time and say, I'm not going to be using your services tonight?
A: I forward from my phone. I can remotely forward it. I can do it directly from my office.
Q: So if you're going to be using the service, you don't have to call them and let them know?
A: No.
Q: You just forward it from your phone?
A: I had my own designated line. I paid for that.
Q: That night that we were talking about earlier, the night before when you spoke to the precinct at 11 p.m. and then there was a call the next day that you allege Aims took your tow, between that time period, were you using the service or were you taking calls yourself?
A: Taking calls myself.
Q: Do you have any way of knowing if the precinct or the police department tried to call you and you didn't have service?
A: They did not call me. I questioned it. I called them back and asked them.
(pp. 201-202)

Q: Is there ever a time when you don't have your cell phone attached to you and you may not have received the call?
A: No. I slept with it.
Q: Then, once you receive the text from your service, do you have to call the
(pp. 277-278)

8. On February 2, 2017, Pilitz was indicted by the Grand Jury for structuring unreported business gross receipts into nominee bank accounts under her control in violation of the Bank Secrecy Act and filing, with the IRS, tax returns containing false information that she signed under the penalty of perjury. United States v Lorraine Pilitz, 17 CR 053(ADS). That indictment was superseded in 2019 to include her personal tax returns.

9. On February 22, 2017 IRS-CI Special Agents and SCPD Detectives arrested Pilitz. During her arrest, the defendant was found in possession of the DEVICE.

Initial Attempt to Search The Device

10. In April 2017, a search warrant for the DEVICE was authorized by Magistrate Judge Arlene R. Lindsay. In Re: The Search of A Silver & White Apple iPhone 6 Assigned Number 516-425-0224, 17 MJ 297. That affidavit in incorporated and made a part of this application. An attempt was made to execute that warrant through transferring the DEVICE into the custody of IRS-CI Computer Investigative Specialist (CIS). Subsequently, CIS agents, after examining the DEVICE, advised the affiant that the IRS-CI did not have the necessary capability to unlock an iPhone 6 with the IOS 10 or higher operating system. CIS advised the affiant that she was unsuccessful in making arrangements with other law enforcement agencies with possible access to resources to unlock the DEVICE. At the time your affiant was advised that there was only a limited number of licenses from Apple permitting agencies to unlock iPhones with IOS 10 or higher. The licenses were retained to be used for a limited number of cases (i.e. national security, etc.). Your affiant has now been advised by an IRS-CI Computer Investigative Specialist that the CIS was now able to unlock the DEVICE, in connection with the current investigation. However, a new search warrant is needed.

PROBABLE CAUSE

11. Based on my knowledge, training, and experience, I know that DEVICE can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the DEVICE. This information can sometimes be recovered with forensic tools.

12. Based on my training, experience, and research, and from consulting the manufacturer's advertisements and product technical specifications and prior examination of

iPhones, I know that DEVICE has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation and it is capable of accessing the internet for purposes of communication such as using Facebook/ Twitter and other similar programs.

13. From the information retrieved from Pilitz' iPhone and multiple digital recorders pursuant to the search warrant executed in June 2014, and Pilitz' statements made during depositions taken during 2008 and 2013 in regards to her civil litigations, I am also aware that Pilitz has a history of regularly recording her conversations with friends, coworkers, paying customers, business associates, and representatives of police departments and other municipal employees. Information that was previously downloaded from Pilitz' iPhone seized during the June 2014 search warrant contained Pilitz contacts, calls and text messages with other individuals. In several text messages Pilitz referred to her business operations and its financial standing. During the above mentioned depositions, Pilitz stated that she regularly received work-related calls and text messages on her personal mobile phone. This Apple Model iPhone 6, identified as the DEVICE, was offered for sale by Apple in September 19, 2014, after Pilitz' prior phone was seized in a prior search warrant. It is anticipate the this phone will contain records of Pilitz' financial and business dealings from 2014 through it's seizure on February 2, 2017, that period includes the period of fraudulent financial conduct that is the basis of current charges in the Indictment.

14. Moreover, based on the contents of Pilitz' prior phone Agents anticipate the DEVICE contains telephone communications and digital recordings that could be used to support Pilitz' on-going involvement and control of her business and substantiate her knowledge of true business income, assist in identifying "off the books" employees not

reflected in any tax or business filings, assist in identifying customers whose payments in cash or check were not deposited through any of Pilitz' business accounts and assist in identifying the source of income structured and diverted into nominee accounts and not reflected on any filed IRS tax returns.

15. This application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how the DEVICE was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence will be in the DEVICE because:

a. Data on an electronic DEVICE can provide evidence of a file that was once on the DEVICE but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the DEVICE that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the DEVICE that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage DEVICE or other external storage media, and the times the DEVICE was in use. Electronic DEVICE can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on an electronic DEVICE can also indicate who has used or controlled the DEVICE. This user attribution evidence is analogous to the search for indicia of occupancy while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, chats, instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last accessed dates) may be evidence of who used or controlled the electronic DEVICE at a relevant time.

c. A person with appropriate familiarity with how an electronic DEVICE works can, after examining this forensic evidence in its proper context, draw conclusions about how DEVICE was used, the purpose of its use, who used it and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on an electronic DEVICE that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, such evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on an electronic DEVICE is evidence may depend on other information stored on the DEVICE and the application of knowledge about how the DEVICE behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. When an individual uses an electronic DEVICE to assist in communications in connecting with money laundering, the individuals electronic DEVICE may generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic DEVICE is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic DEVICE is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic DEVICE used to commit a crime of this type may contain: data that is evidence of how the DEVICE was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

16. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the DEVICE consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer assisted scans of the entire medium, that might expose many parts of the DEVICE to human inspection in order to determine whether it is evidence described by the warrant.

17. Because this warrant seeks only permission to examine the DEVICE already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto the DEVICE. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

18. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that the DEVICE contains evidence of crimes. Accordingly, a search warrant is requested.

WHEREFORE, your deponent respectfully requests that the requested search warrant be issued for A SILVER & WHITE APPLE IPHONE 6 ASSIGNED NUMBER 516-425-0224, IMEI: 359309060188473 UTILILIZED AND SEIZED FROM DEFENDANT LORRAINE SUE PILITZ.

DAVID DARJANIA
Special Agent
IRS - Criminal Investigation

Sworn to before me this
27 th day of September, 2019

/s/ A. Kathleen Tomlinson
THE HONORABLE A. KATHLEEN TOMLINSON
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT B

Particular Things to be Seized

All information obtained from DEVICE will be maintained by the government for the purpose of authentication and any potential discovery obligations in any related prosecution. The information shall be reviewed by the government only for the purpose of identifying and seizing all information described below that constitutes fruits, evidence and instrumentalities of a conspiracy to launder money, in violation of Title 26, United States Code, Sections 7201(1), 7212(a) and Title 31, United States Code, Section 5324.

All records and information on the DEVICE described in Attachment A, including names and telephone numbers, as well as the contents of all call logs, contact lists, text messages, emails (including those sent, received, deleted and drafted), instant messages, photographs, videos, Facebook posts, Internet activity (including browser history, web page logs, and search terms entered by the user), and other electronic media constituting evidence, fruits or instrumentalities of a conspiracy to launder money, in violation of Title 26, United States Code, Sections 7201(1), 7212(a) and Title 31, United States Code, Section 5324 including:

1. Evidence of user attribution showing who used or owned the DEVICE at the time the things described in this warrant were created, edited, or deleted, such as, for example, logs, phonebooks, saved usernames and passwords, documents, and browsing history;

2. Evidence of software that would allow others to control the DEVICE, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

3. Evidence of the lack of such malicious software;

4. Evidence of the attachment to the DEVICE of other storage DEVICEs or similar containers for electronic evidence;

5. Evidence of counter forensic programs (and associated data) that are designed to eliminate data from the DEVICE;

6. Evidence of the times the DEVICE was used;

7. Passwords, encryption keys, and other access DEVICEs that may be necessary to access the DEVICE; and

8. Contextual information necessary to understand the evidence described in this attachment, all of which constitute evidence, fruits and instrumentalities of a conspiracy to launder money, or violations of Title 26, United States Code, Sections 7201(1), 7212(a) and Title 31, United States Code, Section 5324.

BTR
F#2016R0

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

- - - - - - - - - - - - - - - - - - -X

IN THE MATTER OF AN APPLICATION FOR A SEARCH WARRANT FOR:

A SILVER & WHITE APPLE IPHONE 6 ASSIGNED NUMBER 516-425-0224, IMEI 359309060188473 SEIZED FROM DEFENDANT LORRAINE PILITZ (Mobile Device #1), AND

A RED & WHITE OLYPMUS DIGITAL VOICE RECORDER NUMBER 110110076 (Mobile Device #2).

AFFIDAVIT IN SUPPORT OF APPLICATION FOR A SEARCH WARRANT

M. No. 17 MJ 297

- - - - - - - - - - - - - - - - - - -X

EASTERN DISTRICT OF NEW YORK, SS:

DAVID DARJANIA, being duly sworn, deposes and states that he is a Special Agent with the Internal Revenue Service, Criminal Investigation ("IRS-CI"), duly appointed according to law and acting as such.

Upon information and belief, there is probable cause to believe that there is located in A SILVER & WHITE APPLE IPHONE 6 ASSIGNED NUMBER 516-425-0224, IMEI 359309060188473 SEIZED FROM DEFENDANT LORRAINE PILITZ (Mobile Device #1), A RED & WHITE OLYPMUS DIGITAL VOICE RECORDER NUMBER 110110076, SEIZED FROM DEFENDANT LORRAINE PILITZ (Mobile Device #2), as described in Attachment A, for the things described in Attachment B, which constitute evidence, fruits and instrumentalities of filing

false Federal tax returns, corrupt endeavor to obstruct and impede the Internal Revenue Laws and structuring financial transactions in violation of Title 26, United States Code, Sections 7201(1), 7212(a),and Title 31, United States Code, Section 5324.

The source of your deponent's information and the grounds for his belief are as follows:

1. I am a Special Agent with the Internal Revenue Service - Criminal Investigation. I have worked with the IRS-CI for 7 years. During my tenure at the IRS-CI, I have participated in many investigations involving violations of Tax Laws, Bank Secrecy Act and other related offences. In the course of those investigations, I have analyzed various financial records, conducted physical surveillance, monitored undercover operations, interviewed and debriefed cooperating witnesses and confidential informants. As a result of my training and experience, I am familiar with the techniques and methods of operation used by individuals involved in such criminal activity to conceal their activities from detection by law enforcement authorities.

2. I am familiar with the facts and circumstances of this investigation from: (a) my personal participation in this

investigation, (b) reports made to me by other law enforcement authorities, (c) interviews of witnesses, and (d) review of other records and reports.

3. Because this affidavit is being submitted for the purpose of establishing probable cause to search, I have not included every detail of every aspect of the investigation. Rather, I have set forth only those facts that I believe are necessary to establish probable cause. The information set forth below is based upon my experience and training as a law enforcement officer with the IRS-CI, my review of documents and other evidentiary items, debriefing of witnesses, and my discussions with other law enforcement officers. Unless specifically indicated, all conversations and statements described in this affidavit are related in substance and in part only.

BACKGROUND

4. Since February 2011, the Federal Taskforce comprised of IRS-CI Special Agents and Suffolk County Police Department ("SCPD") Detectives were assisting the U.S. Attorney's Office ("USAO") with a Grand Jury investigation of a marijuana grow and distribution network that produced and distributed large quantity of hydroponically grown marijuana and

related money laundering activity in the Eastern District of New York, including Nassau and Suffolk Counties.

5. In October 2013, during arraignment and bail hearing following the arrest of James W. Ford ("Ford"), Lorraine Pilitz, AKA Lorraine Christie, AKA Lorraine Storms, AKA L.S. Christie-Pilitz ("Pilitz") identified herself as Ford's girlfriend and "off-the-books" employer. Ford was convicted in February 2017, after a jury trial, of possession of hydroponically grown marijuana with the intent to distribute. U.S. V Ford, 13 Cr 605(LDW).

6. Pilitz represented herself as a sole owner and operator of several corporations/companies that provide tow and auto-body repair services from several locations in Nassau and Suffolk Counties.

7. In the months following Ford's October 2013 arrest, IRS-CI Special Agents and SCPD Detectives obtained additional information from various sources that indicated that Pilitz was structuring hundreds of thousands of dollars through business and personal bank accounts she controlled.

8. In the Spring of 2014, several search warrants were executed at Pilitz residence, her business locations, and other locations involving Pilitz's relatives which were believed

to have evidence. Recovered in those warrants were multiple records of conversations conducted by Pilitz with others. Pilitz, through her various counsel, indicated she regularly recorded conversations with third-parties without their knowledge.

9. On February 2, 2017, Pilitz was indicted for conduct from 2009 through 2015 by the Grand Jury for structuring unreported business gross receipts into nominee bank accounts under her control in violation of Bank Secrecy Act and filing with the IRS false tax returns. Those false tax returns were prepared in 2015. United States v Lorraine Pilitz, 17 CR 053(BTR). The structured cash was used, in part, to purchase commercial property at 295 East Montauk Highway, Lindenhurst, New York which Pilitz currently uses for varied towing and auto repair business operations. The investigation into Pilitz' current business operations continues.

10. On February 22, 2017, pursuant to an arrest warrant issued by U.S. Magistrate Judge Anne Y. Shields, federal agents arrested Pilitz. During her arrest, the defendant was found in possession of Mobile Device #1 and Mobile Device #2.

11. Based on my training, experience, and research, and from consulting the manufacturer's advertisements and product

technical specifications and prior examination of iPhones, I know that Mobile Device #1 has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation and it is capable of accessing the internet for purposes of communication such as using Facebook/MySpace and other similar programs.

12. Based on my training, experience, and research, and from consulting the manufacturer's advertisements and product technical specifications and prior examination and utilization of digital voice recorders, I know that the Mobile Device #2 has capabilities that allow it to make and store multiple audio recordings.

13. From the information retrieved from Pilitz' iPhone and multiple digital recorders pursuant to the search warrant executed in June 2014, and Pilitz' statements made during depositions taken during 2008 and 2013 in regards to her civil litigations, I am also aware that Pilitz, has a history of regularly recording her conversations with friends, coworkers, paying customers, business associates, and representatives of police departments and other municipal employees. Information that was previously downloaded from Pilitz' phone call seized during the June 2014 search warrant contained records of Pilitz

cell phone relevant contacts, calls and text messages with other individuals, which have evidentiary value, of her associations and potential criminal communications. In several text messages Pilitz referred to her business operations and its financial standing. During the above mentioned civil depositions, Pilitz stated that she regularly received work-related calls and text messages on her personal mobile phone. Pilitz' telephone communications and digital recordings support Pilitz' on-going involvement and control of her business and substantiate her knowledge of true business income and may serve as indirect evidence of her intent to structure the income into nominee accounts and file with the IRS tax returns containing false information.

14. Based on my knowledge, training, and experience, I know that Mobile Device #1 and Mobile Device #2 are capable of storing large amounts of information for an extended period of time. Indeed, information relative to the logistics and contacts needed to prepare the false tax return, prepared in 2015, could easily still exist on the Mobile Device #1. Similarly, things accessed via the Internet are typically stored for some period of time on the Mobile Device #1. This information can sometimes be recovered with forensics tools.

15. This application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how Mobile Device #1 was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence will be found in Mobile Device #1 because:

a. Data on an electronic MOBILE DEVICE #1, such as an iPhone, can provide evidence of a file that was once on the device but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the MOBILE DEVICE #1 that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the Mobile Device #1 that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage or other external storage media, and the times the MOBILE DEVICE #1 was in use. Electronic devices can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on an electronic device can also indicate who has used or controlled MOBILE DEVICE #1. This user attribution evidence is analogous to the search for indicia of occupancy while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, chats, instant messaging logs, photographs, the presence or absence of malware,

and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the electronic device at a relevant time.

c. A person with appropriate familiarity with how an electronic device works can, after examining this forensic evidence in its proper context, draw conclusions about how MOBILE DEVICE #1 was used, the purpose of their use, who used it, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on an electronic device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, such evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on an electronic device, such as MOBILE DEVICE #1, is evidence may depend on other information stored on the MOBILE DEVICE #1 and the application of knowledge about how MOBILE DEVICE #1 behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. I know that when an individual uses an electronic device the MOBILE DEVICE #1 may generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic MOBILE DEVICE #1 is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic MOBILE DEVICE #1 is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic MOBILE DEVICE #1 used to commit a crime of this type may contain: data that is evidence of how the MOBILE DEVICE #1 was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

16. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of MOBILE DEVICE #1 and MOBILE DEVICE #2 consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium that might expose many parts of MOBILE DEVICE #1 and MOBILE DEVICE #2 to human inspection in order to determine whether it is evidence described by the warrant.

17. Because this warrant seeks only permission to examine MOBILE DEVICE #1 and MOBILE DEVICE #2 already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion into any protected area to obtain MOBILE DEVICE #1 and MOBILE DEVICE #2. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

18. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that on MOBILE DEVICE #1 and MOBILE DEVICE #2 may contain evidence of crimes. Accordingly, a search warrant is requested.

WHEREFORE, your deponent respectfully requests that the

requested search warrant be issued for A SILVER & WHITE APPLE IPHONE 6 ASSIGNED NUMBER 516-425-0224,IMEI 359309060188473 SEIZED FROM DEFENDANT LORRAINE PILITZ (Mobile Device #1), AND A

RED & WHITE OLYPMUS DIGITAL VOICE RECORDER NUMBER 110110076 (Mobile Device #2) UTILIZED AND SEIZED FROM DEFENDANT LORRAINE PILITZ.

DAVID DARJANIA
Special Agent
IRS - Criminal Investigation

Sworn to before me this
3rd day of April, 2019

/s/ Arlene R. Lindsay
THE HONORABLE ARLENE R. LINDSAY
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

Property to Be Searched

The properties to be searched are:

1. A SILVER & WHITE APPLE IPHONE 6 ASSIGNED NUMBER 516-425-0224, IMEI: 359309060188473 AND UTILILIZED AND SEIZED FROM DEFENDANT LORRAINE SUE PILITZ ("MOBILE DEVICE #1") and

2. A RED & WHITE OLYMPUS DIGITAL VOICE RECORDER NUMBER 110110076 ("MOBILE DEVICE #2")

This warrant authorizes the forensic examination of MOBILE DEVICE #1 and MOBILE DEVICE #2 for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Particular Things to be Seized

All information obtained from MOBILE DEVICE #1 and #2 will be maintained by the government for the purpose of authentication and any potential discovery obligations in any related prosecution. The information shall be reviewed by the government only for the purpose of identifying and seizing all information described below that constitutes fruits, evidence of violations of Title 26, United States Code, Sections 7201(1), 7212(a) and Title 31, United States Code, Section 5324.

All records and information on the MOBILE DEVICE #1 described in Attachment A, including names and telephone numbers, as well as the contents of all call logs, contact lists, text messages, emails (including those sent, received, deleted and drafted), instant messages, photographs, videos, Facebook posts, Internet activity (including browser history, web page logs, and search terms entered by the user), and other electronic media constituting evidence, fruits or instrumentalities of violations of Title 26, United States Code, Sections 7201(1), 7212(a) and Title 31, United States Code, Section 5324 including:

1. Evidence of user attribution showing who used or owned the MOBILE DEVICE #1 at the time the things described in this warrant were created, edited, or deleted, such as, for example, logs, phonebooks, saved usernames and passwords, documents, and browsing history;

2. Evidence of software that would allow others to control the MOBILE DEVICE #1, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

3. Evidence of the lack of such malicious software;

4. Evidence of the attachment to the MOBILE DEVICE #1 of other storage devices or similar containers for electronic evidence;

5. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from MOBILE DEVICE #1;

6. Evidence of the times the MOBILE DEVICE #1 and #2 were used;

7. Passwords, encryption keys, and other access MOBILE DEVICE #1 that may be necessary to access MOBILE DEVICE #1; and

8. Contextual information necessary to understand the evidence described in this attachment, all of which constitute evidence, fruits and instrumentalities of violations of Title 26, United States Code, Sections 7201(1), 212(a) and Title 31, United States Code, Section 5324.

As used above, the terms records and information include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.